POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACÍÓN

Documento N°: RSM-ISMS-P-A-CHI-00-SIF
Versión V1.0 de 09-10-2024

Información del Documento

Título:	Política General de Seguridad de la Información
Versión:	1.0
Fecha:	09-10-2024
Documento N°:	RSM-ISMS-P-B-CHI-00-SIF
Clasificación:	Interno
Elaborado por:	Franco Godoy
Propietario del documento:	CISO

Historial de revisión:

N° de serie	Fecha	N° de versión	Actualizado por	Revisado por	Aprobado por
1	09-10-2024	V1.0	Franco Godoy	CISO	Comité de Seguridad de la Información, Ciberseguridad y Tecnología

Distribución:

- Las copias controladas del documento estarán disponibles para todos los empleados de la entidad.
- Se podrán emitir copias no controladas a partes externas con el consentimiento de RSM Chile.

CONTENIDO

1. Introducción

En **RSM Chile SPA**, en adelante, **RSM Chile**, la seguridad de la información es un compromiso integral y global que abarca todas las entidades del grupo. Nuestro **Sistema de Gestión de Seguridad de la Información (SGSI)** está diseñado para proteger la confidencialidad, integridad y disponibilidad de la información en todas las filiales de **RSM Chile**. Este sistema establece un marco común de políticas, procedimientos y controles que garantizan una gestión coherente y efectiva de la seguridad de la información en toda la organización.

La presente **Política de Seguridad de la Información** es el fundamento sobre el cual se basa el **SGSI** de **RSM Chile** y es de aplicación obligatoria para todas las empresas del grupo. Esta política define los principios y directrices que guían la protección de los activos de información en todo el grupo, asegurando que cada entidad dentro de **RSM Chile** gestione la seguridad de la información de manera alineada con los estándares internacionales y las mejores prácticas.

En un entorno de amenazas en constante evolución, **RSM Chile** se compromete a mantener un sistema de gestión de la seguridad de la información que sea adaptable, proactivo y eficaz en la mitigación de riesgos a nivel global. Esta política establece las bases para que todas las empresas del grupo implementen y mantengan controles de seguridad que sean consistentes y alineados con las necesidades operativas y regulatorias de **RSM Chile**.

1.1. Objetivo

El objetivo principal de esta Política es establecer los principios y normas esenciales para la gestión de la seguridad de la información en **RSM Chile**. El fin último es asegurar que todas las entidades de RSM Chile garanticen la protección de la información, minimizando los riesgos no financieros que puedan surgir debido a una gestión ineficaz.

1.2. Alcance

Esta Política es aplicable a todas las entidades del grupo **RSM Chile**, así como a todos sus empleados, contratistas, prestadores de servicios y proveedores. El alcance de esta Política abarca toda la información gestionada por **RSM Chile** y sus asociados, sin importar su formato, medio de almacenamiento, quién la procese o dónde se encuentre, ya sea en formato impreso o electrónico.

Esta Política debe ser conocida y cumplida por todos los empleados, contratistas, prestadores de servicios y proveedores de **RSM Chile**, quienes tienen la responsabilidad de actuar en conformidad con los principios aquí establecidos. La Política estará disponible en la página web corporativa de **RSM Chile** y en un repositorio común, accesible para todos los involucrados.

2. Principios de la Política de Seguridad de la Información

Esta Política está alineada con las mejores prácticas de Seguridad de la Información recogidas en el **Estándar Internacional ISO/IEC 27001:2022**, así como con la legislación vigente en materia de protección de datos personales y otras normativas relevantes para **RSM Chile**.

Los principios básicos que guían esta Política incluyen:

- **Compromiso estratégico:** La seguridad de la información debe contar con el apoyo de todos los niveles directivos de **RSM Chile**, integrándose con otras iniciativas estratégicas para formar un marco de trabajo coherente y eficaz.
- **Seguridad integral:** La seguridad de la información debe ser entendida como un proceso integral que incluye aspectos técnicos, humanos, materiales y organizativos. Debe ser parte de la operativa diaria y aplicarse en todo el ciclo de vida de los sistemas de información.
- **Gestión de riesgos:** La gestión de riesgos es esencial para mantener un entorno controlado, minimizando los riesgos a niveles aceptables a través de medidas de seguridad adecuadas que equilibren la naturaleza de los datos, el impacto, la probabilidad de los riesgos, y la eficacia y el coste de las medidas.
- **Proporcionalidad:** Las medidas de protección, detección y recuperación deben ser proporcionales a los riesgos potenciales y a la criticidad de la información y los servicios afectados.
- **Mejora continua:** Las medidas de seguridad deben ser revisadas y actualizadas periódicamente para adaptarse a la evolución constante de los riesgos y tecnologías de protección.
- **Seguridad por omisión:** Los sistemas deben ser diseñados y configurados para garantizar un nivel adecuado de seguridad desde el inicio.

En **RSM Chile**, la seguridad de la información es responsabilidad de todos los empleados, contratistas, prestadores de servicios y proveedores de servicio quienes deben conocer, comprender y asumir esta Política. La organización establecerá una estrategia preventiva para identificar, mitigar y reevaluar regularmente los riesgos, manteniendo un equilibrio entre el apetito por el riesgo y los umbrales de tolerancia.

3. Compromiso de la Dirección

La Dirección de **RSM Chile**, consciente de la importancia de la seguridad de la información para el éxito de sus objetivos de negocio, se compromete a:

- Promover las funciones y responsabilidades en el ámbito de la seguridad de la información en toda la organización.
- Proveer los recursos necesarios para alcanzar los objetivos de seguridad.

- Fomentar la divulgación y concienciación de la Política entre todos los empleados, contratistas, prestadores de servicios y proveedores.
- Exigir el cumplimiento de esta Política, la legislación vigente y los requisitos regulatorios relacionados con la seguridad de la información.
- Incorporar la seguridad de la información en el proceso de toma de decisiones.

4. Roles y responsabilidades

RSM Chile se compromete a proteger todos los activos bajo su responsabilidad mediante las medidas necesarias, cumpliendo con todas las normativas y leyes aplicables. La gobernanza de la seguridad de la información será transversal en toda la organización, abarcando todas sus filiales. **El Chief Information Security Officer (CISO)** de RSM Chile será el responsable de definir, implementar y monitorear las medidas de ciberseguridad y seguridad de la información, asegurando la aplicación consistente de los controles de seguridad.

El CISO, operando bajo un marco de gobernanza centralizado y transversal, reportará directamente al órgano de gobierno o a la comisión de auditoría, y será el encargado de aplicar los principios de segregación de funciones, además de gestionar la relación con autoridades y grupos de interés en materia de seguridad de la información.

El CISO deberá desarrollar y mantener esta Política, garantizando que se ajuste a la evolución de la organización y a las regulaciones vigentes.

5. Gestión de la Seguridad de los Recursos Humanos

El Departamento de Recursos Humanos de **RSM Chile** deberá gestionar los aspectos de seguridad de la información en todas las fases del ciclo de vida de los empleados, desde la contratación hasta la desvinculación. Esto incluye:

- **Formación y Concienciación: RSM Chile** garantizará que todos los empleados reciban la formación y concienciación adecuadas en materia de seguridad de la información, de acuerdo con las normativas vigentes, poniendo especial énfasis en la confidencialidad y la prevención de fugas de información. Los empleados también serán informados sobre cualquier actualización de las políticas y procedimientos de seguridad.
- **Política de Escritorio Limpio:** Los empleados deberán asegurar que sus áreas de trabajo están libres de documentos o dispositivos que contengan información sensible al finalizar la jornada laboral. Los dispositivos deberán bloquearse al dejar el puesto de trabajo, tanto manualmente como de forma automatizada.

6. Gestión de Activos

RSM Chile deberá identificar e inventariar todos los activos de información necesarios para la operación de los procesos de negocio. El inventario de activos se mantendrá actualizado de manera continua.

- **Clasificación de Activos:** Los activos serán clasificados de acuerdo con el tipo de información que contienen, según lo dispuesto en la sección de clasificación de la información.
- **Responsabilidad de Activos:** Cada activo o elemento de información deberá tener un responsable que garantice su correcta clasificación, protección e inventariado. Este responsable deberá mantener un registro formal de los usuarios autorizados a acceder al activo.
- **Gestión de Dispositivos BYOD: RSM Chile** permite el uso de dispositivos personales (BYOD) para acceder a recursos corporativos, siempre que estos dispositivos cumplan con las mismas medidas y configuraciones de seguridad que los dispositivos corporativos. Los usuarios de dispositivos BYOD serán responsables de su seguridad y deberán mantenerlos actualizados con el software de gestión de dispositivos móviles (MDM) proporcionado por el departamento de TI.

7. Gestión del Ciclo de Vida de la Información

RSM Chile gestionará adecuadamente el ciclo de vida de la información para evitar su uso incorrecto en cualquiera de las fases:

1. **Creación o Recolección:** Registra y almacena información desde su origen, ya sea creada internamente o recibida de fuentes externas.
2. **Distribución:** Gestiona la información creada o recibida, tanto internamente como externamente.
3. **Uso o Acceso:** Regula el acceso autorizado a la información, asegurando que solo personas autorizadas puedan acceder a ella.
4. **Almacenamiento:** Organiza y gestiona la información para garantizar su accesibilidad y seguridad.
5. **Destrucción:** Implementa prácticas para eliminar la información que ha cumplido su período de retención, garantizando su confidencialidad durante el proceso de destrucción.

RSM Chile deberá identificar y aplicar las medidas de seguridad necesarias para asegurar la correcta gestión del ciclo de vida de los activos de información.

8. Gestión de Copias de Seguridad

RSM Chile deberá realizar copias de seguridad periódicas de la información, el software y los sistemas, verificándolas regularmente:

- Las copias de seguridad deberán realizarse al menos semanalmente, y con mayor frecuencia si la información es de alta criticidad.
- Las copias de seguridad deben recibir las mismas protecciones que los datos originales y, siempre que sea posible, deberán estar cifradas.
- Se realizarán pruebas periódicas de restauración de copias de seguridad para asegurar su funcionamiento adecuado. Estas pruebas serán documentadas.

Las copias de seguridad deberán almacenarse en ubicaciones seguras y preferiblemente en centros diferentes a donde se generaron, garantizando la integridad de la información ante posibles incidentes de seguridad, como ataques de ransomware.

9. Clasificación de la Información

RSM Chile establecerá un modelo de clasificación de la información que defina las medidas técnicas y organizativas necesarias para proteger la información en función de su sensibilidad:

- **Tipos de Información:** La información se clasificará en soportes lógicos (digitales) y físicos (documentos impresos y otros medios de almacenamiento).
- **Niveles de Clasificación:** La información se categorizará en niveles como Uso Público, Interno y Confidencial.

10. Control de Acceso

RSM Chile implementará controles de acceso que aseguren que solo usuarios autorizados puedan acceder a la información y sistemas:

- **Requisitos de Negocio:** Los usuarios serán únicos, sin posibilidad de compartir cuentas, y deberán utilizar autenticación de doble factor (MFA) cuando sea posible.
- **Derechos de Acceso:** Los permisos se basarán en la necesidad de saber y el principio de privilegios mínimos, asegurando una adecuada segregación de funciones.

11. Seguridad Física y del Entorno

Las instalaciones de **RSM Chile** donde se ubiquen los sistemas de información deberán estar protegidas mediante controles de acceso físico, sistemas de vigilancia y medidas preventivas para mitigar riesgos como accesos no autorizados, robos, sabotajes y desastres ambientales.

12. Seguridad en el Trabajo en la Nube

RSM Chile mantendrá una política de seguridad en la nube que garantice la confidencialidad, integridad y disponibilidad de la información:

- **Infraestructura:** Asegurar que el proveedor de servicios en la nube monitoriza el entorno y establece controles de acceso robustos.
- **Plataforma y Software:** Seguir las mejores prácticas de seguridad, incluyendo las guías de OWASP y/o SANS25 para la seguridad de aplicaciones.

13. Seguridad en la Operativa

Todos los sistemas de información de **RSM Chile** deberán contar con medidas de seguridad adecuadas que optimicen su nivel de madurez. Las redes se gestionarán y monitorearán adecuadamente para proteger los sistemas y aplicaciones de amenazas.

14. Seguridad en las Telecomunicaciones

RSM Chile asegurará que su arquitectura de red cuenta con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se implementarán controles adicionales para los datos sensibles que circulen por redes públicas.

15. Seguridad en el Ciclo de Vida del Desarrollo de Sistemas

RSM Chile garantizará que todos los procesos de adquisición, desarrollo y mantenimiento de sistemas incorporen requisitos mínimos de seguridad. Se gestionarán las pruebas, los cambios y el inventario de software conforme a las mejores prácticas del sector.

16. Seguridad en los Proveedores

Se evaluará la criticidad de los servicios subcontratados para asegurar que los proveedores cumplen con los requisitos de seguridad establecidos por **RSM Chile**. Los procesos de selección, los acuerdos contractuales y la monitorización de los servicios deberán garantizar la seguridad de la información subcontratada.

17. Gestión de Incidentes

Todos los empleados de **RSM Chile** son responsables de identificar y notificar cualquier incidente que pueda comprometer la seguridad de la información. **RSM Chile** implementará procedimientos de gestión de incidentes que incluyan la categorización, análisis de impacto y escalado de incidentes.

18. Continuidad de Negocio

RSM Chile dispondrá de un Plan de Continuidad de Negocio que garantice la continuidad de los servicios esenciales en caso de crisis. Este plan será revisado y probado periódicamente, e incluirá un Plan de Recuperación ante Desastres para las tecnologías de la información.

19. Cumplimiento Regulatorio

RSM Chile se compromete a cumplir con toda la legislación y normativa aplicable en materia de seguridad de la información. La responsabilidad de este cumplimiento recae en todos los miembros de la organización.

20. Auditorías de Seguridad y Gestión de Vulnerabilidades

RSM Chile realizará auditorías periódicas para identificar vulnerabilidades técnicas en sus sistemas y aplicaciones. Una vez identificadas, se implementarán las medidas correctivas necesarias con un enfoque basado en riesgos.

21. Gestión de Excepciones

Cualquier excepción a esta Política deberá ser registrada e informada al responsable de Seguridad de la Información de **RSM Chile**. Las excepciones se analizarán para evaluar los riesgos y serán aprobadas por los responsables del negocio en conjunto con el peticionario.

22. Sanciones Disciplinarias

El incumplimiento de las obligaciones establecidas en esta Política, así como de las Políticas específicas del Sistema de Gestión de Seguridad de la Información, Procedimientos u otros documentos derivados de estas, será sancionado conforme a las leyes vigentes y aplicables, así como al reglamento interno de orden para los funcionarios de **RSM Chile**.

Para los empleados de **RSM Chile**, el incumplimiento podrá resultar en sanciones disciplinarias que van desde amonestaciones hasta la terminación del contrato laboral, dependiendo de la gravedad de la infracción. Estas sanciones se aplicarán de acuerdo con lo estipulado en el reglamento interno de la organización y en conformidad con la normativa legal vigente.

En el caso de personas que no tengan responsabilidades administrativas dentro de **RSM Chile**, como prestadores de servicios, contratistas o proveedores, y que se encuentren dentro del alcance de esta Política, cualquier incumplimiento podrá resultar en la terminación anticipada del contrato, por incumplimiento de obligaciones contractuales. Esto será sin perjuicio de las responsabilidades civiles y penales que pudieran derivarse de dichas infracciones, las cuales serán perseguidas conforme a la ley.

RSM Chile se reserva el derecho de actuar legalmente contra cualquier individuo o entidad que incumpla con las obligaciones establecidas en esta Política, asegurando así la protección de la información y los activos de la organización.

23. Revisión de la Política

Esta Política será revisada y aprobada anualmente por el Comité de Seguridad de la Información, Ciberseguridad y Tecnología de **RSM Chile**. En caso de cambios significativos en el entorno operativo o en los riesgos, la Política se revisará cuando sea necesario para asegurar que sigue siendo adecuada a la realidad de la organización.

24. Anexos

24.1. Anexo A – Directrices para la clasificación de activos de información

Tipo	*Características*	*Directrices de gestión*
Crítica, Confidencial	La pérdida de este tipo de activos de información: a) tendría un impacto en la competitividad de RSM Chile. b) podría causar un efecto adverso en las finanzas de RSM Chile. *c) RSM Chile podrían enfrentarse a la interrupción / pérdida de oportunidades.*	*Esta información deberá estar encriptada y protegida por contraseña cuando se almacene o se transmita.*
		El acceso a esta información estará estrictamente limitado y siempre controlado.
		Esta información no debe dejarse sin vigilancia cuando no se utilice, si se encuentra desatendida, se lo notificará al CISO.
		La distribución y reproducción de esta información será estrictamente limitada y estará sujeta a aprobación.
		Los ejemplares impresos de esta información se protegerán bajo llave cuando no se utilicen.
		La información en formato electrónico se almacenará siempre en la unidad de red asignada al departamento / grupo de trabajo correspondiente.
		Siempre se debe guardar una copia de seguridad de la información en formato electrónico, de preferencia en una ubicación externa.
		Los ejemplares impresos también se escanearán y se mantendrán preferentemente en un lugar externo como copia de seguridad.
		El propietario será responsable de la clasificación, calificación y evaluación del riesgo asociado a esta información.
		Arriesgar esta información se considerará como un incidente y está sujeto a estrictas medidas disciplinarias.
		El contenedor de esta información se considerará tan crítico como la información que se guarda en él.
		Esta información se puede compartir (si se requiere y aprueba) con un tercero, si se ha firmado un acuerdo de confidencialidad.
		Esta información se eliminará según los procedimientos de eliminación de información.

Interno	*La categoría "Interno" de activos de información incluye la información que se debe conservar dentro de la empresa, restringida al departamento de origen, los departamentos receptores autorizados y a sus empleados.*	*El acceso a esta información estará limitado únicamente a todos los empleados de RSM Chile.*
		Esta información está destinada solo para uso interno, aunque puede compartirse con terceros mediante un acuerdo de confidencialidad.
		La copia de seguridad de esta información se basará en las necesidades de la empresa y en la indicación del propietario.
		El propietario será responsable de la clasificación, calificación y evaluación del riesgo asociado a esta información.
		Esta información se eliminará según los procedimientos de eliminación de información.
Público	*La categoría pública de activos de información incluirá anuncios públicos, artículos de la empresa, noticias en los medios de comunicación publicados por RSM Chile, así como documentos de investigación para consumo público, sitios web de interés público, etc. Poner en riesgo estos activos no causará ninguna pérdida financiera / de reputación, pero la empresa puede tener que enfrentar la opinión pública / de los medios de comunicación.*	*Garantizar la precisión e integridad de la información (creada por RSM Chile) cuando se ponga a disposición del público.*
		La información que se haga pública está sujeta a la aprobación correspondiente.

EXENCIÓN DE RESPONSABILIDAD

consentimiento previo por escrito del Comité de Seguridad de la Información, Ciberseguridad y Tecnología (ISOC) de RSM Chile. Aquello que no se indique específicamente en este documento no se considerará implícito de ninguna manera. Aquello que no se indique específicamente en este documento no se considerará implícito de ninguna manera.

RSM Chile Auditores Ltda.

Cruz del Sur 133, 4° Piso
Las Condes
Santiago.
T: + (56) 232 539 050

El Bosque Norte 500, Oficina 1002
Las Condes
Santiago.
T: + (56) 232 539 050

THE POWER OF UNDERSTANDING
ASSURANCE | TAX | CONSULTING